20th National Information Systems Security Conference

Role-Based Risk Analysis

Amit Yoran*
Lance J. Hoffman**

The George Washington University
Department of Electrical Engineering and Computer Science

CURRENT ADDRESSES:

* Defense Information Systems Agency
701 South Courthouse Road
Arlington, VA 22204-2199
amit@assist.mil : (800) 719-6029

**Dept of EE and CS, The George Washington University
801 22nd St NW
Washington D.C. 20052
Hoffman@seas.gwu.edu : (202) 994-5513

Role-Based Risk Analysis

Outline

- Traditional Risk Analysis
- Need for Further Development
- Role-Based Methodology
- Advantages of Role-Based Analysis
- Future Research

Traditional Risk Analysis

1. Identify Assets
2. Determine Vulnerabilities
3. Estimate Likelihood of Exploitation
4. Compute Annual Expected Loss
5. Survey New Controls
6. Project Annual Savings of Controls

Modifications to Traditional Risk Analysis

- Osgood - Tandem Threat Methodology Models Successions of Threats
-
- Jaworski - Additive Analysis Across Multiple Sites in Networked Environments

- Drake and Morse - Models a Security Breach over Time

Need for Further Development

- Business Requirements Differ From Military
- As Elsewhere, Shift from Automation to Efficiency
- Traditional Models Don’t Address Outsourced Distributed Risk Analysis
-

Role-Based Risk Analysis Methodology: Terminology

Role:

- Function an entity plays
- Defined by responsibilities and expectations
- Allows for customization of model

  Example: Information Owner

Actor:

- Fills one (or more) roles

  Example: Corporation as an information owner

Role-Based Methodology: Additional Stages

1. *Define the roles.*
2. *Identify the actors.*
3. Identify assets from actor's perspective.
4. Determine vulnerabilities.
5. Estimate likelihood of exploitation.
6. Compute expected annual loss.
7. Survey applicable controls and their costs.
8. Project annual savings of controls.

Role-Based Methodology:Example

Stage 1. Role Definition Stage 2. Identify Actors

ROLE	ACTOR
Information Owner	Company A
Information Holder	Company B, Company A
Protecting Agent	Company C, Compnay D, and Company A
Acting Agent	Company E
Sponsor	Individual F

A computer software engineering firm (Company A) provides an investment banking company (Company B) copies of its financial information. It also maintains this financial information on its own network for periodic updating. Company B retains this information on their corporate network. Company B also hires an information security consulting firm (Company C) to protect the information on their network. Company C implements a firewall to protect Company B's network. The firewall used is developed by Company D. Company A's in-house data automation department provides protection for the information on its network. Finally, an individual F, that works for a competitor, hires Company E to retrieve information on Company A's finances.

Role-Based Risk Analysis Methodology: Typical Threats and Associated Roles

Threat		IO	IH	PA
Information leakage				
Disclosure		✓		✓
Malicious programs (trapdoor, Trojan horse)				✓
Dysfunctional system controls			✓	✓
Physical intrusion			✓	
Eavesdropping		✓		✓
Traffic analysis		✓		✓
Emanations analysis		✓		✓
Masquerade		✓		✓
Scavenging			✓	✓
Integrity violation				
Malicious programs (trapdoor, Trojan horse)				✓
Dysfunctional system controls		✓	✓	✓
Modification		✓	✓	✓
Denial of service				
Malicious programs (trapdoor, Trojan horse)				✓
Natural disaster		✓	✓	✓
Accidental destruction		✓	✓	
Resource flooding			✓	
Communications flooding				✓
Theft			✓	✓
Malicious destruction		✓		✓
Totals	19	10	9	16

IO = Information Owner
IH = Information Holder
PA = Protecting Agent

Note: No risk analysis is provided for Acting Agent or Sponsor.

Role-Based Methodology: Typical Countermeasures and Associated Roles

Countermeasure		IO	IH	PA
Statement of non-disclosure		✓		
Encryption		✓		✓
Authentication		✓		✓
Non-repudiation		✓		✓
Digest				✓
Time stamping			✓	✓
Outsourced security consulting		✓	✓	
Documented Trusted Computing Base		✓	✓	
Defined and enforced security policy		✓		✓
Audit			✓	✓
Access controls			✓	✓
Firewalls				✓
Intrusion detection systems				✓
Personnel controls		✓	✓	✓
System verification procedures			✓	✓
Redundancy/fault tolerance			✓	✓
Archives		✓		
Totals	17	9	8	13

IO = Information Owner
IH = Information Holder
PA = Protecting Agent

Note: No risk analysis is provided for Acting Agent or Sponsor.

Advantages of Role-Based Analysis

- Appropriateness to Distributed Business Environments
-
- Reduction in Analysis Complexity
-
- Non-Traditional Fields of Analysis

Role-Based Risk Analysis: Future Work

- Role Evolution
- Avoiding Potentially Parochial Views
- Developing Legal Standards of Care for Each Role
- Overcoming Responsibility Avoidance